# 安全性质的可结合性*

余祥宣 马建平 张江陵

(华中理工大学计算机科学与工程系 武汉 430074)

**摘要** 安全系统是由许多子系统组成,每一子系统都必须满足一定的安全性质,但这不能保证由这些子系统组合而成的系统也是安全的,即组合的系统不一定也满足给定的安全性质,所以要求系统的安全性质满足可结合性.该文介绍了一种新的基于无干扰概念的多级安全性质,并证明了它是可结合的.

**关键词** 安全性质,可结合性,无干扰,多级安全.

**中图法分类号** TP391

一个大的计算机系统是由若干独立的小系统结合而成的.如果每一个子系统是安全的,那么,由这些子系统结合成的大系统是否也是安全的?答案是否定的.[1,2]系统的开发与验证也是分模块、分系统进行的.因此,如果模块或子系统的安全性质满足可结合性质,则由这些模块和/或子系统组合成的系统也会满足相应的安全性质.

## 1 安全性质

### 1.1 系统模型

我们把为计算系统抽象地定义为状态机.

**定义1.** 一个多级系统是一个状态机 $M=(Q,I,O,L,T,\delta,q_0)$,其中 $Q$ 是状态集合,$I$ 是输入事件集合,$O$ 是输出事件集合,$L$ 是安全级的集合,且$(L,\leqslant)$是一个格,$T$ 是时钟事件集合,$\delta: Q\times I^*\to Q\times O^*$ 是下一状态函数,$q_0$ 是初始状态.其中 $I^*$ 和 $O^*$ 是事件序列;$S$ 是主体集;对任意 $q\in Q, a\in I, seq\in I^*$,$\delta$ 满足下列等式

$$\delta(q,\varnothing)=(q,\varnothing);$$

$$\delta(q,a\circ seq)=\delta(\delta(q,a),seq).$$

我们把系统中的事件分为3类:输入事件 $I$、输出事件 $O$ 和系统时钟事件 $T$,每一类事件都有安全级.输入事件的安全级由输入事件的主体的安全级确定,输出事件的安全级由接受事件的主体安全级确定,系统时钟事件的安全级是最低安全级.我们用 $E=I\cup O\cup T$ 表示系统中所有事件的集合.对任意 $s\in S, e\in E$,$l(s)$,$l(e)$分别表示主体 $s$、事件 $e$ 的安全级.此外,对于任意 $e\in I\cup O$,我们用 $s(e)$ 表示激发(若 $e\in I$)或接受(若 $e\in O$)事件 $e$ 的主体,$t(e)$ 表示事件 $e$ 发生时所对应的时钟事件和时间.若 $e$ 是时间事件,则激发主体是系统时钟,接受主体是系统中所有的主体;其发生时间是其本身(即 $t(e)=e$),用大于零的正整数表示.

为了讨论系统行为的方便,下面引入系统的迹的概念.

**定义2.** 系统 $M$ 的一个迹具有如下的形式

$$(q_0,\varnothing)(q_1,e_1)(q_2,e_2)\ldots(q_n,e_n),$$

其中 $q_0$ 表示 $M$ 的初态,对于 $e_i\in I, q_i\in Q$,存在 $e_j\in I, q_j\in Q$,使得 $\delta(q_i,e_i)=(q_j,e_j)$,$(0\leqslant i<j\leqslant n)$.对任意 $i,j(0\leqslant i<j\leqslant n)$,要求 $t(e_i)<t(e_j)$,即事件 $e_i$ 发生在事件 $e_j$ 之前(假设没有两个事件是同时发生的).

从定义可以看出,系统 $M$ 的迹是$(Q\times E)^*$中的元素.对于迹中的$(q_i,e_i)$,$0\leqslant i\leqslant n$,主体能观察到的是 $e_i$,所以,可定义$(q_i,e_i)$的安全级 $l((q_i,e_i))=l(e_i)$.另外,对于$\varnothing$(在本文中表示空集、空序列和不存在事件),定义它的安全级 $l(\varnothing)$为系统的最低级.

### 1.2 安全性质

系统 $M$ 首先要满足多级安全的简单安全和星性质[3],其次还必须保证高级主体不能通过隐通道把高安全级信息

---

* 作者余祥宣,1942年生,教授,主要研究领域为密码学,计算机安全,计算机算法.马建平,1966年生,博士,主要研究领域为数据安全,形式化方法,安全协议.张江陵,1930年生,教授,博士导师,主要研究领域为信息存储与I/O并行处理,信息安全.

本文通讯联系人:余祥宣,武汉 430074,华中理工大学计算机科学与工程系

本文1997-02-26收到原稿,1997-07-03收到修改稿

传递给低安全级主体，也就是要保证不存在存储隐通道和尽量降低定时隐通道的带宽. 基于新无干扰概念[4]，系统 $M$ 要满足安全性质，即，仅当主体 $a$ 的安全级低于或等于主体 $b$ 的安全级时，主体 $a$ 的行为才能干扰主体 $b$ 的行为.

为了形式化表示安全性质，我们先定义函数 *purge*.

**定义** 3. (1) $purge_t: L\times E^*\to E^*$ 定义为：对 $a\in E, seq\in E^*, l\in L$,

$purge_t(l,\varnothing)=\varnothing$;

$purge_t(l,a\circ seq)$=if $l\geqslant l(a)$ then $a\circ purge_t(l,seq)$ else $t(a)\circ purge_t(l,seq)$.

(2) $purge_t: L\times(Q\times E)^*\to(Q\times E)^*$ 定义为：对 $a\in Q\times E, seq\in(Q\times E)^*, l\in L$,

$purge_t(l,\varnothing)=\varnothing$;

$purge_t(l,a\circ seq)$=if $l\geqslant l(a)$ then $a\circ purge_t(l,seq)$ else $t(a)\circ purge_t(l,seq)$.

函数 *purge* 的功能是把输入序列或迹中的所有与高级和不可比级的主体行为有关的事件剔除，只保留 $l$ 级主体能够观察和引发的事件.

**定义** 4. (安全性质)如果对任意 $M$ 的输入序列 $seq\in I^*$，任意安全级 $l\in L$，有

$$purge_t(l,\delta(q_0,seq))=purge_t(l,\delta(q_0,purge_t(l,seq))),$$

则 $M$ 是多级安全的.

这一定义的含义是针对 $l$ 级的任一主体，高级和/或不可比级主体的行为对他的行为没有影响，并且他不可能观察到高级和/或不可比级主体的行为及其结果.

## 2　可结合性

可结合性是安全性质的重要特性，它的重要性已在很多文献[1,2,5]中讨论过，本文不再赘述. 系统的组合方式如图 1所示. 组合系统的迹由参与组合的两个系统的部分事件序列组成，两个系统之间的通信事件变成了内部事件. 我们假定组合系统具有统一的系统时钟，即参与组合的系统的时钟事件相同.

**定义** 5. 对任意两个多级系统 $M_1=(Q_1,I_1,O_1,L_1,T_1,\delta_1,q_{01})$ 和 $M_2=(Q_2,I_2,O_2,L_2,T_2,\delta_2,q_{02})$，如果 $L_1=L_2, T_1=T_2, (I_1\cap O_2)\cap(I_2\cap O_1)=\varnothing$，对任意 $e\in E_1\cap E_2, l_1(e)=l_2(e)$ 且 $t_1(e)=t_2(e)$，则多级安全系统 $M_1$ 和 $M_2$ 是可结合的.

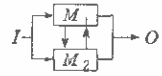

图1　组合方式

**命题**. 如果两个多级系统 $M_1=(Q_1,I_1,O_1,L_1,T_1,\delta_1,q_{01})$ 和 $M_2=(Q_2,I_2,O_2,L_2,T_2,\delta_2,q_{02})$ 是可结合的，则组合系统 $M=M_1\parallel M_2$ 是个多级系统. 其中 $M_1\parallel M_2$ 定义为

(1) $Q=Q_1\cup Q_2$;

(2) $I=(I_1-O_2)\cup(I_2-O_1)$;

(3) $O=(O_1-I_2)\cup(O_2-I_1)$;

(4) $L=L_1=L_2$;

(5) $T=T_1=T_2$;

(6) $\delta(q,\varnothing)=(q,\varnothing)$, $\delta(q,a\circ seq)$=if $a\in I_1$ then $\delta(\delta_1(q,a),seq)$ else $\delta(\delta_2(q,a),seq)$;

(7) $q_0=\{q_{01},q_{02}\}$, $\delta(q_0,a)$=if $a\in I$ then $\delta_1(q_{01},a)$ else $\delta_2(q_{02},a)$. (证明略)

**定理**. 对任意两个多级系统 $M_1=(Q_1,I_1,O_1,L_1,T_1,\delta_1,q_{01})$ 和 $M_2=(Q_2,I_2,O_2,L_2,T_2,\delta_2,q_{02})$，如果 $M_1$ 和 $M_2$ 都满足安全性质，即都是多级安全的，则 $M_1$ 和 $M_2$ 的组合系统 $M=(Q,I,O,L,T,\delta,q_0)$ 也是多级安全的.

证明：即要证明对任意 $M$ 的输入序列 $seq\in I^*$，任意安全级 $l\in L$，有

$$purge_t(l,\delta(q_0,seq))=purge_t(l,\delta(q_0,purge_t(l,seq))).$$

按输入序列 $seq$ 的长度归纳，即可证明上面的等式成立.

## 3　结　论

本文介绍了一种基于新的无干扰概念[4]的安全性质，与其他无干扰性质[1,2,5]的区别在于，它显式地考虑了系统时钟事件，便于分析系统的定时隐通道. 这种安全性质是可结合的，这一特性保证了它与其他可结合的无干扰安全性质一样，可用于分析和验证安全系统的安全性.

### 参考文献

1　McCullough D. Noninterference and the composability of security properties. In: David Bailey ed. Proceedings of the Sympo-

sium on Security and Privacy. Oakland: IEEE Computer Society Press, 1988. 177～186

2 McCullough D. A hookup theorem for multilevel security. IEEE Transactions on Software Engineering, 1990,16(6):563～568

3 Bell D E, LaPadula L J. Secure computer systems: unified exposition and multics interpretation. Technical Report MTR-2997, Bedford: The Mitre Corp., 1976

4 马建平. 一种新的无干扰模型[硕士论文]. 华中理工大学,1994
(Ma Jian-ping. A new noninterference model[M. S. Thesis]. Huazhong University of Science and Technology, 1994)

5 Goguen J A, Meseguer J. Security policies and security models. In: Roger R Schell ed. Proceedings of IEEE Symposium on Security and Privacy. Oakland: IEEE Computer Society Press, 1982. 11～20

## Composability of Security Property

YU Xiang-xuan MA Jian-ping ZHANG Jiang-ling

(*Department of Computer Science and Engineering Huazhong University of Science and Technology Wuhan* 430074)

**Abstract** A secure system consists of many sub——systems, even though every one of those sub-systems satisfies a certain security property, the composed system may not be secure, i. e. the composition maybe not satisfy the security property. It does mean that the security property should be composable. In order to solve such problems, a new multilevel security property based on a new concept of noninterference is introduced and the seurity property is proven to be composable in this paper.

**Key words** Security property, composability, noninterference, multilevel security.